U.S. Cyber Command Academic Engagement Strategy Webinar
Wednesday, October 13, 2021

MR. FREDERICK: Good afternoon, everyone. I'm Dave Frederick, the Executive Director of U.S. Cyber Command. I'm honored today to be here at DreamPort to launch our new Academic Engagement Strategy. I should note up front that this event is going to be recorded and we plan on posting the recording afterward.

I want to thank all of you for taking time today to join the webinar and for your interest in partnering. Cyber is truly the ultimate team sport, and we get a lot of value from our academic partnerships.

Let's go ahead and turn to the slides and get started.

Let me mention that we're really looking forward to your questions at the end of the briefing. So as I'm going over the content, take the time to go ahead and submit your questions in the chat tool and at the end we will go through as many questions as we can. If we run out of time, we'll respond to any other questions after the event by updating our program information.

So I'm going to start off today with a Cyber Command 101. In a way, this is kind of a vocabulary lesson. The military and the cyber community loves acronyms, so I want to try to demystify the organization, our strategy and our technology approach. We'll then focus on our academic engagement goals and end with announcing our new partnership framework called the Cyber Command Academic Engagement Network.

Cyber Command has three main missions. The first is to defend the Department of Defense's networks, called the DODIN. The DODIN consists of over 4 million computing devices. As you can imagine, this mission is a daunting one given the complexity of the environment and the fact that we have nation-state adversaries trying to hack the network every day. This mission is assigned to a subordinate headquarters, known as the Joint Force Headquarters-DODIN.

Our second mission is to defend the nation against significant cyber attack. We always conduct this mission as part of a whole-of-government effort, and partner very closely with other agencies such as CISA, FBI, and within the DOD, U.S. Northern Command and NSA. Our role is to conduct operations outside the United States, imposing cost on our adversaries in foreign cyberspace. The Cyber National Mission Force is the organization responsible for this mission.

Our third mission is supporting the joint force, and in this role, Cyber Command provides cyber options to other joint force commanders and we provide cyber-defense operations.

So, for example, if there was a crisis in the Pacific region, U.S. Indo-Pacific Command would rely on Cyber Command and our forces to both defend their networks and also provide offensive cyber operations for their campaign. This mission is conducted by four subordinate Joint Force Headquarters, which are aligned with the military services.

I want to talk a bit about the Cyber Mission Force without boring you today with an organizational chart. I've already mentioned our three main missions. I do want to note, you'll hear us refer to Cyber Command in short form as CYBERCOM. Each military service also has a service cyber command, and they're responsible for training and managing the cyber teams that form the core of our combat capability. On the map I've highlighted some of our primary locations, although we do have units in other locations besides these four spots.

Shifting to strategy, the United States is engaged in strategic competition with China and Russia. Both nations conduct broad campaigns in cyberspace targeting the United States and our allies. The cornerstone of America's defense is deterrence, and Cyber Command has a key role to play in ensuring our adversaries understand that the costs of aggression would far outweigh the benefits. Cyber Command performs this role via a persistent engagement strategy where we can test adversary efforts to gain an advantage on the United States every day. We develop capabilities, conduct planning and execute operations to conduct – to enable a range of options for the President and joint force commanders.

There are two components to our persistent engagement strategy: enable and act. And a great example of persistent engagement in action is the joint teamwork we performed to protect the 2020 elections with the National Security Agency. In that mission, we enabled DHS and FBI by sharing unique information that enabled them to assure election systems were secure and also counter foreign cyber disinformation. Cyber Command also conducted two dozen operations in foreign cyberspace in order to prevent foreign threats from interfering or influencing the 2020 election.

Before shifting to our academic goals, I want to briefly describe our mission capabilities concept, known as the Joint Cyber Warfighting Architecture, or JCWA. JCWA includes four major programs that are delivering our big-data platform, our command and control systems, our training environment and our cyber access capabilities. In addition, JCWA contains a portfolio of tools, cyber weapons and sensors that enable both our offensive and defensive missions.

A key focus of our academic engagement will be mission innovation, and so I'd briefly describe what JCWA looks like in 2021, but our key question is what should JCWA look like in 2031? How will artificial intelligence, 5G, quantum computing change the environment and change our mission needs? How can academia help us imagine this future?

To organize our efforts, we’ve established four goals that we’ll focus on for the next two years, and in each case, given our limited resources, we will prioritize actions to support accomplishment of these goals. Relatively speaking, our academic engagement efforts will be more limited than the broader government programs that are managed by DHS, NSA and government research labs.

Focusing on our first goal, we want to engage and inspire students to consider careers in DOD, both in the military and as civilians. We really want to broaden awareness of some great internship programs that Cyber Command runs, as does the service commands. In teamwork with NSA, we’re also engaging on the DOD Cyber Institute’s pilot. This program was funded by Congress initially for six universities in order to better prepare students for cyber careers in the department.

We are also going to kick off a voluntary guest lecturing program, offering both focused lecturing at specific institutions and also broader offerings via webinars. Our capacity will be limited, so we’ll be really looking forward for – looking forward to your feedback and your applications so we can help design our program and focus on what’s most meaningful and helpful for the academic community.

As I mentioned before, innovation is going to be critical to us, and our Acquisition and Technology Directorate, also referred to as the J9, runs the innovation process for the whole Cyber Mission Force. A key part of that process is development of innovation challenge problems, which today we share with the Defense Innovation Unit, In-Q-Tel and the research labs around DOD. In the future, we want to do a more effective job at sharing this list with academia, and we also want to support a limited number of capstone projects through technical mentoring. As an example, right now we’ve got a project where we’re supporting midshipmen at the U.S. Naval Academy who selected one of our innovation problems related to malware analysis. So we have some technical experts helping the midshipmen throughout the academic year on this project.

I do want to highlight that DOD is kicking off a new university consortium for cybersecurity later this year that will be managed by the National Defense University. This consortium will focus on DOD’s hardest cyber research problems, and we look forward to partnering with NDU and engaging with the broader universities through this consortium.

Finally, before moving off innovation, I want to go ahead and share three main priorities we have for the next year where we would like new ideas from academia and assistance in developing new capabilities. One is understanding and disrupting the ransomware ecosystem. The second is protecting U.S. elections from foreign disinformation. And thirdly, understanding how to develop zero – and deploy zero-trust in complex cloud-based environments.

Our third goal aims to expand partnerships with academia to take – to build better relationships and take advantage of the deep expertise in academia about adversaries' cyber strategies and organizations. As an extension of DIA's analytic partnership program, our Intelligence Directorate, or the J2, will host expert engagements on a quarterly basis and also sponsor a limited number of research projects each year. In fact, we just inked an agreement with Harvard – Harvard's undergraduate research program. Students are going to investigate foreign military adversary organizations and share their findings at the end of the academic year.

Our final goal focuses on engaging a diverse group of academics on military cyber strategy and the role of the military in the context of broader public-private efforts. Cyberspace continues to evolve rapidly, and we will seek opportunities to critically engage on military strategy and doctrine with a broad group of universities.

Also part of this effort is coordinated senior leader engagements. So we receive a number of requests for senior leaders to meet with faculty and students to discuss our mission, discuss our organization, and we look forward to supporting those to the extent we can.

Let's move on now to the details on the how. So we're going to organize our communications with academia in the form of an Academic Engagement Network. This is going to provide a consistent and transparent communications channel between U.S. Cyber Command, the service cyber commands and academic institutions. We are inviting both the DOD key schools such as the National Defense University, College of Information and Cyberspace, and the service academies, as well as U.S. non-federal institutions, to join the Academic Engagement Network. You'll see that the eligibility is pretty straightforward, and in our application form we are requesting a little bit more information than that so we can design our program and focus on priorities that are of mutual benefit.

To apply to the academic network, we will – you need to go to our website and clink on the links I've got displayed there and create an application – I'm sorry, an access network account. To do that, you need a passcode, so this is important for you to write down. The passcode to create the academic account is "persistent engagement".

I want to close by highlighting what we have planned in the upcoming months. We will start with broad offerings to all participants in the form of three webinars. The first will focus on cyber strategy. We're going to hold a second one that will be a deep dive on our innovation program and focus in on a handful of innovation challenge problems. And the third will be how to hack cyber hiring, and this webinar will be focused for your students and really help them understand all the great internship opportunities they have and how to apply for positions within the – with Cyber Command and the service cyber components. We'll also provide some exposure to ROTC and opportunities within the ROTC program to pursue a cyber role.

Around February our Intelligence Directorate will invite institutions to participate in a seminar focused on foreign adversary disinformation, and that opportunity will include both a chance to serve on a panel as well as just dial in and listen to the event.

With that, let's go ahead and move to Q&A.

Okay, so the first question I've got is: "Will this initiative tie in with the Centers of Academic Excellence programs from NSA and DHS?"

So we work obviously very closely with NSA on the CAE programs, and we are taking great care not to duplicate the work they're doing. We encourage universities that are members of CAE as well as those that aren't, if there's a good matchup with your interests, your programs and our academic goals, to please apply to our engagement network.

Next question. Okay, the question is: "How can we partner with Cyber Command?"

So as I noted, and you can go to our website right now – if you go to cybercom.mil you'll be able to navigate down into our partnership section and find the application links. The key is to apply to this Academic Engagement Network, and again, just to reinforce the passcode when you create that account is "persistent engagement". So the first step is to sign up. We're going to wait until the 15th of November and then take a look at all the initial applicants as a whole, verify eligibility, and then sometime around the 15th you'll start hearing from us. You may get – we may offer some of the webinars a bit earlier than that, but most likely the webinars will kick off sometime after the 15th. But in any case, if you're in this webinar you're going to hear back from us unless you don't apply to be part of the network.

Next question. "Where can I find a listing of some of the needed joint force research and innovation areas?"

Okay, this is a great question. So for CYBERCOM's innovation challenge problems, they are posted on our website, and so you can go there right now if you go into the cybercom.mil webpage and see the list of the innovation challenge problems that we developed in 2020. We have just kicked off a refresh of those problems, but I'll you, when you look at the list you'll see they're really hard problems; they're not stale. But we will be updating the list probably in the late spring of 2022.

In terms of the broader joint force research needs, it's something to keep an eye out with the different research labs in the military and with DARPA.

The next question is: "Where can we find more on the NDU Consortium for Cybersecurity?"

So I don't want to get too far ahead of the National Defense University, but they do have a website already. So if you I think google maybe UC2 or Consortium for Cybersecurity, you should be able to find their initial landing page. I understand they're going to launch the consortium sometime around December, and that'll give you the basic context of the plan if you go to their webpage at this point. More to follow on that from the NDU team.

Okay. "Academia is usually focused on basic research on the five-plus-year horizon. You talked about needs for the next one to two years, like ransomware. Is U.S. Cyber Command intending to prioritize near-term tactical problems? If you're not providing funding, what should schools expect from UCC?"

Great questions. So I highlighted three near-term problems that we're interested in. If you have research work underway in those areas, we'd like to hear from you. But that is not the only priority. So you'll see from our innovation list it's a much broader set of problems with that, and many of them are certainly problems that are going to take more than five years to solve. I will say we're more focused on applied research and innovation than basic research, so there is a difference there.

In terms of funding, I should emphasize we do not issue grants. That's – grant issuance in the department is done by research labs and by NSA. But we are offering opportunities to engage with our technical workforce and to really hear our perspective on that. We do influence the requirements for grants as well as, potentially in the future, might have some contract-based opportunities to engage us. If we do have a case where we have a need that we'll contract out, the contracting process won't be handled through the engagement network, it'll be handled through the normal contracting methods to make sure that it complies with all the laws and regulations.

The next question is: "Will engagement activities also involve classified research or projects?"

Another great question. So, potentially. We do have both our unclassified innovation list and challenge problem list, and we do – we separately have some classified problems. We won't be funding creation of SCIFs or investment in the infrastructure to enable a university to start classified research, but if you are a university that already has an ability to conduct classified research there may be opportunities for that in the future to work with us on some of our problems.

Next question. "How will this program provide distinctive pathways to help individuals gain employment with DOD agencies? Currently, NSA administers an underfunded DOD cyber scholarship program. Does this initiative collaborate with this program?"

So for Cyber Command as a warfighting headquarters, we basically set the requirements for the workforce, but the hiring and the scholarships are handled by the military services and by DOD. And so what – but what we're going to try to do is make it easier for your students and faculty that's advising students to understand what's out there. So one of the early webinars will really focus on this question of what type of internships are available, and how can students apply to that, how – what type of new employee development programs are available, which a number of the services offer as does the command headquarters – how can they apply, and then how do they navigate the federal government jobs process.

In terms of scholarships, I'll take a note of that and we'll make sure as well to highlight the scholarship for service opportunities and some of the other opportunities in the Intelligence Community where students could pursue a cyber career with a scholarship aspect.

The next question. Okay, this next question is a little confusing to me, but it's basically asking how does our program relate to the consortium of universities to advice the Secretary of Defense on cybersecurity matters.

So that consortium is the University Consortium for Cybersecurity that I mentioned earlier. So the relationship we will have with the National Defense University is we'll be sharing our challenge problems, our research problems with them and having an influence on the priorities and working very closely with NDU and the consortium as they reach out to schools to share the DOD's hardest problems.

Next question. "Air Force Cyber College is developing a series of case studies for teaching at DOD or civilian schools in response to a joint staff call. How can the Air Force Cyber College best get the word out to prospective writers for our program?"

So I would encourage Air Force Cyber College – we look forward to partnering with you and we hope you'll join our engagement network, for one, and I would ask for the team there to reach back to us after this call and we can talk about ways that we can get the word out and support you in that endeavor.

Next question. "Are you interested in applied research for workforce development?"

The answer on that one is very simple. Yes. I think a key area for us is how do we provide training and how do we incentivize and develop the workforce in cyber. So you can expect to see problems in that space from us, and potentially that might be an area that the UC2 program investigates in the future as well.

Next question. "Can two-year colleges participate too? Is this program applicable for community college or geared to higher-level students?"

Excellent question. I would say – I could understand why the way we briefed it community colleges may not have seen themselves as much in the proposal. But absolutely, we are hoping that community colleges will apply. I think the question for you as a community college is the alignment of your activities with our academic goals. Community college offers an excellent opportunity for education, early education that can help prepare people for roles in the military as well as DOD civilian careers. And so we encourage the community colleges to consider applying. If it turns out as we engage that your interests are actually more aligned with what CISA is working on or what NSA is doing, we can help connect the dots between you and some of our colleagues around the community.

Next slide. “Can you provide any additional insight with regard to the command’s interest in engaging academia regarding cyber strategy? Any examples?”

Yeah. So just briefly, when you look at how quickly cyberspace is evolving, how our adversaries are adapting to changes in the environment and also to policy moves that the United States takes, the questions we always have is: What’s the military’s role? How can we be as effective as possible? How do we need to adapt strategically to support the President and to support joint force commanders as effectively as possible?

Right now a major focus for us is integrated deterrence and understanding the role Cyber Command will play in that context. What are the lessons learned from the last few years under persistent engagement that’s going to inform us as we continue to evolve our approach to defending the United States?

Next question. “What are you looking for in terms of levels, duration, master’s versus certificates, et cetera? Can you expand on workforce development, skills, training needs?”

So that’s a pretty broad question. I would share with you that – kind of two focus areas that I would highlight. One is, how do we prepare students as they’re completing college to be ready as possible to be competitive for DOD careers? How do we actually make sure they even understand what’s available and what kind of roles we have? It’s a very competitive market for cybersecurity skills, and we want to make sure that students understand at both the graduate and undergraduate levels kind of the roles that are available within the DOD for cyber missions and some of the unique things they can do here.

So, for example, our integrated operator role, which is performed both by enlisted personnel and officers, is a great example where the degree of education, the amount of education can vary quite a bit, but people can do a truly unique role in support of the country and receive some incredible training once they’re on board and within the force. So we have a very capable training program, and what we want to do is continue to influence the educational approach in the educational institutions to make the matchup between newly graduating students and our needs as complementary as possible.

Next question. "Is the CYBERCOM and NDU academic engagement effort a consolidation of service-level cyber engagements or distinct?"

Okay, let me split that out. So the National Defense University consortium will be very focused initially on DOD's highest-priority cyber research needs. So it's a bit different.

The Cyber Command Academic Engagement Network is in fact encompassing of the service-level commands, so Army Cyber, Air Force Cyber, Marine Forces Cyber. Each one of those cyber commands runs their own internship programs. They engage universities and colleges to meet their assigned mission needs. What we're trying to do is provide a better framework so that universities kind of know where to go and orchestrate the work that we're doing much more closely with the Marines, Coast Guard, Navy, Army and Air Force. So it is an all-encompassing engagement network that should help you communicate with us and the service commands more effectively. It will not replace or diminish anything that's happening in the service-level cyber components.

Next slide – pardon me, next question. "Is CYBERCOM tasked with looking at over the horizon for personnel development 10 to 15 years from today, funding, experience, et cetera?"

So yeah, that's a – it's really hard, right? If you look at how fast technology changes, to look 15 years out is pretty challenging. But yes, we certainly have a role in communicating to DOD's CIO, to DOD personnel about what our needs are for personnel development, and are constantly looking at how do we better train and focus education and training activities to support our personnel.

So I think one of the areas we'll look at, for example, is new technology. So as new technologies emerge – application of artificial intelligence is a good example of that – how does that change our needs? I mean, are there areas that we're training people for today that we no longer have to train them for? Do we need to shift them in a different direction to deal with the environment and changes in adversary behavior?

Next question. "Is the application due November 1 or November 15?"

So we're shooting for a November 15 submission date for the initial tranche of applications. It will be rolling, a rolling application after that, but we want to take a snapshot November 15th, and that'll let us get things going in terms of communicating back out to the universities consistently and allow our team to kind of go through the eligibility process. We're going to go and look at your application. We'll be looking at just verifying eligibility, but you're also going to see questions in the application about your interest areas for guest lecturing and mentorship, and we're trying to look also at some of the faculty research, learn a little bit about for research institutions what type of work your faculty is doing. But we're going to bring all that together and use that to try to steer and prioritize.

For our guest lecturing program and capstone support, there's going to be a limited number of events we can support per year, and so we want to make it as meaningful as possible to the faculty and the students of the institutions.

So November 15th is the key date, but again, if you're a little bit late on that it's not going to be the end of the world. It will be rolling, but we may not kind of get back to you until a month or two later if you don't submit by the November 15th date.

Next slide. "Are you going to share the slides from this presentation?"

We're not going to push the slides out independently, but what we are doing is posting the webinar, the recorded video that you're seeing, which will give you a way to see the slides, and they'll be out on our web at some point in the next few weeks on our webpage.

Next question. Okay. The good news for me, since I was starting to get hoarse, is there are no more questions right now. But we've got a little bit of time left, and so if people want to post any more questions in the chat, let us know and we'll keep the chat open for, say, another 30 minutes and we'll answer them over email just back to you directly. And again, we're going to take these questions and use it to also help kind of update our program information to help folks understand what we're trying to accomplish.

And with that, again, I want to thank all of you for taking time out of your day to join us for this webinar, for your interest in working with U.S. Cyber Command, and for what you're doing to help prepare the next generation of Americans that are going to help us in the cyber mission.

So again, as one more final reminder, as you apply, you're going to need a passcode to complete the application and that passcode is the word "persistent" space – not the word "space," a space – and then the word "engagement". So "persistent engagement". So again, we look forward to your applications and thanks again for taking time with us today. Have a great day.

# # # #